In the claims:

For the Examiner's convenience, all pending claims are presented below with changes shown.

1.   (Currently Amended) A method comprising:

encrypting, based ~~least in part~~ upon at least one key, one or more respective portions of ~~input~~write data to generate one or more respective portions of ~~output~~ encrypted write data to be stored in one or more locations in storage; ~~and at least one of:~~

generating, based ~~at least in part~~ upon the one or more respective portions of the ~~output~~encrypted write data, check data to be stored in the storage; and

selecting the one or more locations so as to permit the one or more respective portions of the ~~output~~encrypted write data to be distributed among two or more storage devices comprised in the storage.

2.   (Currently Amended) The method of claim 1, wherein:

the storage comprises a redundant array of independent disks (RAID); and

the check data comprises one of parity data and a copy of the ~~output~~encrypted write data.

3.   (Currently Amended) The method of claim 1, further comprising:

storing the at least one key in memory; and

in response, ~~at least in part,~~ to an attempt to tamper with the at least one key, erasing the at least one key from the memory.

4.   (Currently Amended) The method of claim 1, further comprising:

determining, based at least in part upon one or more credentials, whether to permit

execution of one or more operations involving the storage.

5.   (Currently Amended) A method comprising:

receiving a read request;

retrieving one or more respective portions of the encrypted data from a plurality of

storage devices comprised in the storage; and

decrypting, based least in part upon at least one key, one or more respective portions

of input the encrypted read data retrieved from one or more respective locations in storage to

generate one or more respective portions of output read data; and at least one of:

generating check data to be stored in the storage, the check data being generated

based at least in part upon the one or more respective portions of the input data; and

retrieving the one or more respective portions of the input data from a plurality of

storage devices comprised in the storage.

6.   (Currently Amended) The method of claim 5, further comprising:

receiving a request to retrieve requested data from the storage, the requested data

comprising the output data; and prior to the decrypting of the one or more respective portions

of the input encrypted data, determining, based at least in part upon one or more credentials,

whether the request is authorized.

7. (Currently Amended) The method of claim 6, further comprising:

generating, ~~at least in part,~~ the at least one key based ~~at least in part~~ upon at least one of one or more tokens and one or more passwords.

8. (Currently Amended) The method of claim 5, wherein:

the storage also stores metadata; and

the method further comprises encrypting the metadata based ~~at least in part~~ upon the at least one key.

9. (Original) The method of claim 8, wherein:

the metadata comprises partition information.

10. (Currently Amended) An apparatus comprising:

circuitry to encrypt, based ~~least in part~~ upon at least one key, one or more respective portions of ~~input~~write data to generate one or more respective portions of ~~output~~encrypted write data to be stored in one or more locations in storage;

the circuitry also being capable of ~~at least one of~~:

generating, based ~~at least in part~~ upon the one or more respective portions of the ~~output~~encrypted write data, check data to be stored in the storage; and

selecting the one or more locations so as to permit the one or more respective portions of the ~~output~~encrypted write data to be distributed among two or more storage devices comprised in the storage.

Docket No. 42P17160
Application No. 10/686,410   -4-

11.   (Currently Amended) The apparatus of claim 10, wherein:

the storage comprises a redundant array of independent disks (RAID); and

the check data comprises one of parity data and a copy of the ~~output~~encrypted write

data.

12.   (Currently Amended) The apparatus of claim 10, wherein:

the circuitry is also capable of storing the at least one key in memory; and

in response, ~~at least in part,~~ to an attempt to tamper with the at least one key, erasing

the at least one key from the memory.

13.   (Currently Amended) The apparatus of claim 10, wherein:

the circuitry is also capable of determining, based ~~at least in part~~ upon one or more

credentials, whether to permit execution of one or more operations involving the storage.

14.   (Currently Amended) An apparatus comprising:

circuitry to receive a read request, retrieve one or more respective portions of the

encrypted data from a plurality of storage devices comprised in the storage and decrypting,

based upon at least one key, one or more respective portions of the encrypted read data

retrieved from storage to generate one or more respective portions of ~~output~~ read data

~~decrypt, based least in part upon at least one key, one or more respective portions of~~

~~input~~write ~~data from storage to generate one or more respective portions of output~~encrypted

write ~~data; the circuitry being capable of at least one of: generating check data to be stored in~~

~~the storage, the check data being generated based at least in part upon the one or more~~

~~respective portions of the input~~ <ins>write</ins> ~~data; and retrieving the one or more respective portions~~

~~of the input~~ <ins>write</ins> ~~data from a plurality of storage devices comprised in the storage.~~

15.   (Currently Amended) The apparatus of claim 14, wherein the circuitry is also

capable of:

~~receiving a request to retrieve requested data from the storage, the requested data~~

~~comprising the output data; and~~ prior to the decrypting of the one or more respective portions

of the ~~input~~ <ins>encrypted</ins> data, determining, based ~~at least in part~~ upon one or more credentials,

whether the request is authorized.

16.   (Currently Amended) The apparatus of claim 15, wherein:

the circuitry is also capable of generating~~, at least in part,~~ the at least one key based ~~at~~

~~least in part~~ upon at least one of one or more tokens and one or more passwords.

17.   (Currently Amended) The apparatus of claim 14, wherein:

the storage also stores metadata; and the circuitry is also capable of encrypting the

metadata based ~~at least in part~~ upon the at least one key.

18.   (Original)   The apparatus of claim 17, wherein:

the metadata comprises partition information.

Docket No. 42P17160
Application No. 10/686,410   -6-

19. (Currently Amended) An article comprising a storage medium having stored therein instructions that when executed by a machine result in the following:

encrypting, based ~~least in part~~ upon at least one key, one or more respective portions of ~~input~~write data to generate one or more respective portions of ~~output~~ encrypted write data to be stored in one or more locations in storage; ~~and at least one of:~~

generating, based ~~at least in part~~ upon the one or more respective portions of the ~~output~~encrypted write data, check data to be stored in the storage; and

selecting the one or more locations so as to permit the one or more respective portions of the ~~output~~encrypted write data to be distributed among two or more storage devices comprised in the storage.

20. (Currently Amended) The article of claim 19, wherein:

the storage comprises a redundant array of independent disks (RAID); and

the check data comprises one of parity data and a copy of the ~~output~~encrypted write data.

21. (Currently Amended) The article of claim 19, wherein the instructions when executed by the machine also result in:

storing the at least one key in memory; and

in response, ~~at least in part,~~ to an attempt to tamper with the at least one key, erasing the at least one key from the memory.

Docket No. 42P17160
Application No. 10/686,410   -7-

22.   (Currently Amended) The article of claim 19, wherein the instructions when executed by the machine also result in:

determining, based ~~at least in part~~ upon one or more credentials, whether to permit execution of one or more operations involving the storage.

23.   (Currently Amended) An article comprising a storage medium having stored therein instructions that when executed by a machine result in the following:

receiving a read request;

retrieving one or more respective portions of the encrypted data from a plurality of storage devices comprised in the storage; and

decrypting, based ~~least in part~~ upon at least one key, one or more respective portions of ~~input~~ the encrypted read data retrieved from ~~one or more respective locations in~~ storage to generate one or more respective portions of ~~output~~ read data; ~~and at least one of:~~

~~generating check data to be stored in the storage, the check data being generated based at least in part upon the one or more respective portions of the input data; and~~

~~retrieving the one or more respective portions of the input data from a plurality of storage devices comprised in the storage.~~

24.   (Currently Amended) The article of claim 23, wherein the instructions when executed by the machine also result in:

~~receiving a request to retrieve requested data from the storage, the requested data comprising the output data; and~~ prior to the decrypting of the one or more respective portions of the ~~input~~ encrypted data, determining, based ~~at least in part~~ upon one or more credentials,

whether the request is authorized.

25.   (Currently Amended) The article of claim 24, wherein the instructions when executed

by the machine also result in:

generating, at least in part, the at least one key based at least in part upon at least one

of one or more tokens and one or more passwords.

26.   (Currently Amended) The article of claim 23, wherein:

the storage also stores metadata; and

the instructions when executed by the machine also result in encrypting the metadata

based at least in part upon the at least one key.

27.   (Original)   The article of claim 26, wherein:

the metadata comprises partition information.

28.   (Currently Amended) A system comprising:

a circuit board comprising a circuit card slot and a circuit card that is capable of being

inserted into the circuit card slot, the circuit card comprising circuitry, the circuitry being

capable of encrypting, based least in part upon at least one key, one or more respective

portions of inputwrite data to generate one or more respective portions of outputencrypted

write data to be stored in one or more locations in storage;

the circuitry also being capable of at least one of:

Docket No. 42P17160
Application No. 10/686,410   -9-

generating, based at least in part upon the one or more respective portions of

the outputencrypted write data, check data to be stored in the storage; and

selecting the one or more locations so as to permit the one or more respective

portions of the outputencrypted write data to be distributed among two or more

storage devices comprised in the storage.

29.   (Currently Amended) The system of claim 28, wherein: the circuitry comprises an

input/output (I/O) processor, and

non-volatile memory that is capable of storing the at least one key; and

the circuitry is capable of detecting-an attempt to tamper with the at least one key,

and in response, at least in part, to the attempt, erasing the at least one key from the memory.

30.   (Original)   The system of claim 29, wherein:

the circuit board also comprises a host processor coupled to the circuit card slot via a

bus, and one or more token memories to store one or more tokens; and

additional circuitry to read one or more additional tokens stored in a removable token

memory after the removable token memory is inserted into a token reader.

31.   (Currently Amended) A system comprising:

a circuit board comprising a circuit card slot and a circuit card capable of being

inserted into the circuit card slot, the circuit card comprising circuitry to receive a read

request, retrieve one or more respective portions of the encrypted data from a plurality of

storage devices comprised in the storage and decrypting, based upon at least one key, one or

Docket No. 42P17160
Application No. 10/686,410   -10-

more respective portions of the encrypted read data retrieved from storage to generate one or more respective portions of read data ~~decrypt, based least in part upon at least one key, one or more respective portions of input data from storage to generate one or more respective portions of output data;~~

~~the circuitry also being capable of at least one of:~~

~~generating check data to be stored in the storage, the check data being generated based at least in part upon the one or more respective portions of the input data; and~~

~~retrieving the one or more respective portions of the input data from a plurality of storage devices comprised in the storage.~~

32. (Original)   The system of claim 31, further comprising:

an input/output (I/O) controller coupled to a redundant array of independent disks (RAID); and

a bus via which the controller is coupled to the circuitry.

33. (Original)   The system of claim 32, wherein:

the circuit board also comprises a host processor coupled to the slot and the controller.

Docket No. 42P17160
Application No. 10/686,410   -11-

PAGE 14/18 * RCVD AT 4/23/2007 5:18:06 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/7 * DNIS:2738300 * CSID:3037406962 * DURATION (mm-ss):10-18